UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

LISA SMITH AND ELISA STROFFOLINO, on behalf of themselves and all others similarly situated, Plaintiffs, v. **APRIA HEALTHCARE LLC** Defendant.	**Case No. 1:23-cv-01003-RLY-KMB** **JURY TRIAL DEMANDED**

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Lisa Smith and Elisa Stroffolino, individually and on behalf of all similarly situated persons, allege the following against Apria Healthcare LLC ("Apria" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs brings this class action against Apria for its failure to properly secure and safeguard Plaintiffs' and other similarly situated Apria patients' personally identifiable information ("PII") and protected health information ("PHI"), including personal, medical, health insurance information, and financial information, and Social Security numbers (the "Private Information"), from criminal hackers.[1]

[1] https://www.hipaajournal.com/apria-healthcare-breach-affects-up-to-1-8-million-individuals/ (last visited on May 23, 2023); *see also* https://apps.web.maine.gov/online/aeviewer/ME/40/bf218a4e-1ffd-4f14-a74d-

2. Apria, based in Indianapolis, Indiana, is a provider of home medical equipment for sleep apnea and other medical conditions, serving medical providers and patients across the country.

3. On or about September 1, 2021, Apria received notification regarding access to its systems by an unauthorized third party and, through its investigation, determined that a threat actor had access to its systems from April 5, 2019 to May 7, 2019, and again from August 27, 2021 to October 10, 2021 (the "Data Breach").[2]

4. Apria filed official notice of a hacking incident on or around May 22, 2023. Under state and federal law, organizations must report breaches that impact PHI within at least sixty (60) days. On or around May 22, 2023, Apria also posted a notice of the Data Breach on its website, informing its patients of the hacking incident, though not providing sufficient detail regarding the same. Apria has also recently sent Data Breach notice letters to impacted patients on or around June 6, 2023, which Plaintiffs received (all three forms of notice are collectively referred to herein as the "Notice"). Thus, Apria waited in some cases over three years to disclose the Data Breach to impacted victims.

5. As a result of this delayed response, Plaintiffs and "Class Members" (defined below) had no idea for *years* that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. This risk will remain for their respective lifetimes.

6. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not

3d34aec8d6c7.shtml (noting that, "Financial Account Number or Credit/Debit Card number (in combination with security code, access code, password or PIN for the account" were also impacted) (last visited on May 23, 2023).

[2] *See* file:///C:/Users/tbean/Downloads/Apria%20HIPAA%20Notification%20Letter%20PDF%20(1).pdf (last visited on May 23, 2023).

limited to, Social Security numbers, financial information, and PHI that Apria collected and maintained.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. There has been no assurance offered by Apria that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

9. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiffs bring this class action lawsuit to address Apria's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

11. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Apria, and thus Apria was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

12. Upon information and belief, Apria failed to properly monitor and properly implement security practices with regard to its computer network and systems that housed the Private Information. Had Apria properly monitored its networks, it would have discovered the Breach sooner.

13. Plaintiffs' and Class Members' identities are now at risk because of Apria's negligent conduct as the Private Information that Apria collected and maintained is now in the hands of data thieves and other unauthorized third parties.

14. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

II. PARTIES

15. Plaintiff Lisa Smith is, and at all times mentioned herein was, an individual citizen of the State of Illinois.

16. Plaintiff Elisa Stroffolino is, and at all times mentioned herein was, an individual citizen of the State of California.

17. Defendant Apria is a Delaware limited liability company with its principal place of business in Indianapolis, Indiana.

III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of

interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Apria. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has jurisdiction over Apria because Apria operates in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Apria has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Apria's Business and Collection of Plaintiffs' and Class Members' Private Information

21. Apria is a provider of home medical equipment for sleep apnea and also provides pharmaceutical services and equipment and supplies for wound care and diabetes. Apria is headquartered in Indianapolis, Indiana, serving medical providers and patients across the country in 275 locations.[3] In 2021 alone, Apria served over 2.05 million patients.[4] Apria also employs roughly 6,500 individuals.[5]

22. As a condition of receiving its products and services, Apria requires that its customers and patients entrust it with highly sensitive personal and health information. In the ordinary course of receiving services from Apria, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

23. In its Privacy Policy and HIPAA Privacy Notice (collectively, the "Privacy Policy"), Apria promises its patients that any disclosures of its patients' Private Information falling outside of the excepted circumstances set forth therein would be done "only with your written

[3] *See* https://www.apria.com/ (last visited on May 30, 2023).
[4] *Id*.
[5] *Id*.

authorization."[6] However, Plaintiffs' and Class Members' Private Information has been disclosed without their written authorization as a result of the Data Breach.

24. Through its Privacy Policy, and in light of the highly sensitive and personal nature of the information Apria acquires and stores with respect to its patients, Apria promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

25. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Apria assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

26. Plaintiffs and Class Members relied on Apria to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members

27. According to Defendant's Notice and other publicly available information, on or about September 1, 2021, Apria received notification regarding access to its systems by an unauthorized third party and, through its investigation, determined that a threat actor had access to

[6] *See* https://www.apria.com/hubfs/GEN-4539_Form_Notice-Privacy-Practices_04-22_v2_FNL.pdf (last visited on May 30, 2023).

its systems from April 5, 2019 to May 7, 2019, and again from August 27, 2021 to October 10, 2021.[7]

28. Apria filed official notice of the Data Breach on or around May 22, 2023 and, upon information and belief, sent direct notice to Plaintiffs and Class Members on or around the same time. Thus, Apria waited, in some cases, over four years to disclose the Data Breach to impacted victims.

29. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including PHI, financial information, and Social Security numbers.

30. Apria had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

31. Plaintiffs and Class Members provided their Private Information to Apria with the reasonable expectation and mutual understanding that Apria would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

32. Apria's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

33. Apria knew or should have known that its electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

[7] *See* file:///C:/Users/tbean/Downloads/Apria%20HIPAA%20Notification%20Letter%20PDF%20(1).pdf (last visited on May 23, 2023).

34. Apria was on notice that companies in the healthcare industry are susceptible targets for data breaches.

35. Apria was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[8]

36. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[9]

37. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[10] In 2022, the largest growth in compromises occurred in the healthcare sector.[11]

---

[8] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on May 30, 2023).

[9] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on May 30, 2023).

[10] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on May 30, 2023).

[11] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on May 30, 2023).

38. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[12]

39. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[13]

40. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[14]

41. As a healthcare goods and services provider, Apria knew, or should have known, the importance of safeguarding its patients' Private Information, including PHI, entrusted to it, and

---

[12] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on May 30, 2023).

[13] *Id*.

[14] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on May 30, 2023).

of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Apria's patients as a result of a breach. Apria failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. Apria Failed to Comply with HIPAA

42. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

43. Apria's Data Breach resulted from a combination of insufficiencies that indicate Apria failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Apria's Data Breach that Apria either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

44. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

45. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

46. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

47. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

48. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

49. Based upon Defendant's Notice to Plaintiffs and Class Members, Apria reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

50. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

51. Apria reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

52. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

53. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

54. Apria reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

55. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

56. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

57. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

58. In addition, Apria's Data Breach could have been prevented if Apria had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

59. Apria's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Apria creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

60. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required Apria to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

61. Because Apria has failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Apria's approach to information security is adequate and appropriate going forward. Apria still maintains the PHI and other highly sensitive PII of its current and former patients, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

E. Apria Failed to Comply with FTC Guidelines

62. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

63. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection

system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

64. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

65. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. As evidenced by the Data Breach, Apria failed to properly implement basic data security practices. Apria's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

67. Apria was at all times fully aware of its obligation to protect the Private Information of its patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Apria Failed to Comply with Industry Standards

68. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

69. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Apria include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

70. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

71. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

72. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

G. Apria *Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information*

73. In addition to its obligations under federal and state laws, Apria owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Apria owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

74. Apria breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Apria's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its patients Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

75. Apria negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

76. Had Apria remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

77. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Apria.

H. Apria Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

78. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[15] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the

[15] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on May 30, 2023).

ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

79. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

80. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

81. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

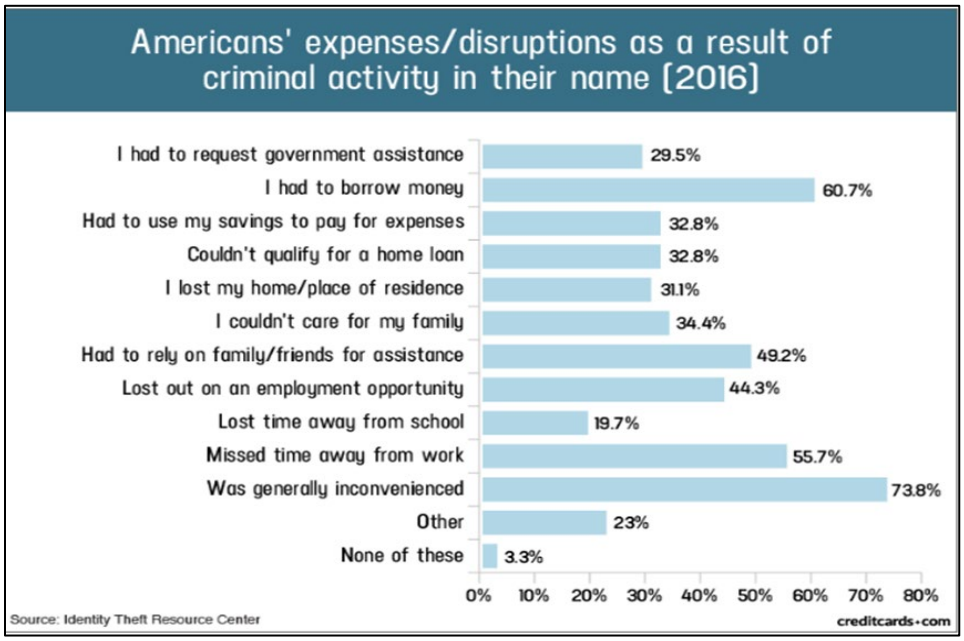
82. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

83. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[16] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

84. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[16] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited May 30, 2023).

85. In fact, a study by the Identity Theft Resource Center[17] shows the multitude of harms caused by fraudulent use of PII:



86. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[18]

87. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

88. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[19]

---

[17] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on May 30, 2023).

[18] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on May 30, 2023).

[19] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on May 30, 2023).

89. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

90. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[20]

91. The ramifications of Apria's failure to keep its patients' Private Information secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

92. Here, not only was sensitive medical information compromised, but insurance information and Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

93. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is

[20] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on May 30, 2023).

misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[21]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

94. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

95. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. Plaintiffs' and Class Members' Damages

96. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

97. As a requisite to receiving medical equipment and services from Defendant, Plaintiffs provided their Private Information to Defendant and trusted that such would be safeguarded according to state and federal law. For example, both Plaintiffs Smith and Stroffolino entrusted their Private Information to Defendant when ordering medical equipment from Defendant. Upon receipt, the Private Information was entered and stored onto Defendant's network and systems.

[21] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited May 30, 2023).

98. Plaintiffs' and Class Members' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

99. As a direct and proximate result of Apria's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

100. Further, as a direct and proximate result of Apria's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

101. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

102. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

103. Plaintiffs and Class Members also lost the benefit of the bargain they made with Apria. Plaintiffs and Class Members and/or their insurance overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price paid by Plaintiffs and Class Members (or on their behalf) to Apria was intended to be used by Apria to

fund adequate security of Apria's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

104. Additionally, as a direct and proximate result of Apria's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and insurance statements for unauthorized activity for years to come.

105. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

106. Plaintiffs and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases due to the active and robust legitimate marketplace for Private Information that exists. In 2019, the data brokering industry was worth roughly $200 billion.[22] In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to other companies.[23] Consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[24]

107. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and

[22] See Data Coup, https://datacoup.com/.
[23] *What is digi.me?, DIGI.ME,* https://digi.me/what-is-digime/ (last visited Jan. 16, 2023).
[24] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Jan. 16, 2023).

diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

108. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

109. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Apria, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

110. As a direct and proximate result of Apria's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

111. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

112. Specifically, Plaintiffs propose the following Nationwide Class and State Subclasses (collectively referred to herein as "Class Members," the "Class," or the "Classes"), subject to amendment as appropriate:

Nationwide Class

> All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach for which Apria provided notice to Plaintiffs and other Class Members beginning on or around June 6, 2023.
>
> **Illinois Subclass**
>
> All residents of Illinois whose Private Information was actually or potentially accessed or acquired during the Data Breach for which Apria provided notice to Plaintiffs and other Class Members beginning on or around June 6, 2023.
>
> **California Subclass**
>
> All residents of California whose Private Information was actually or potentially accessed or acquired during the Data Breach for which Apria provided notice to Plaintiffs and other Class Members beginning on or around June 6, 2023.

113. Excluded from the Classes are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

114. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

115. The proposed Classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

116. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of roughly 1.8 million patients of Apria whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Apria's records, Class Members' records, publication notice, self-identification, and other means.

117. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Apria engaged in the conduct alleged herein;

b. Whether Apria's conduct violated the FTCA, HIPAA, or the state statutes invoked below;

c. When Apria learned of the Data Breach

d. Whether Apria's response to the Data Breach was adequate;

e. Whether Apria unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

f. Whether Apria failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Apria's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Apria's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Apria owed a duty to Class Members to safeguard their Private Information;

j. Whether Apria breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Apria had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether Apria breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether Apria knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of Apria's misconduct;

p. Whether Apria's conduct was negligent;

q. Whether Apria's conduct was *per se* negligent;

r. Whether Apria was unjustly enriched;

s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

118. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Apria. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there

are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

119. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

120. Predominance. Apria has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Apria's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

121. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Apria. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

122. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Apria has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

123. Finally, all members of the proposed Class are readily ascertainable. Apria has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Apria.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

124. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

125. Apria knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

126. Apria's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

127. Apria knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Apria was

on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

128. Apria owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Apria's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA, the FTCA, and California's Confidentiality of Medical Information Act ("CMIA");

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

129. Apria's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

130. Apria's duty also arose because Defendant was bound by industry standards to protect its patients' confidential Private Information.

131. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Apria owed them a duty of care to not subject them to an unreasonable risk of harm.

132. Apria, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Apria's possession.

133. Apria, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

134. Apria, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

135. Apria breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA, HIPAA, and/or the CMIA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

136. Apria acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

137. Apria had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Apria with their Private Information was predicated on the understanding that Apria would take adequate security precautions to protect it. Moreover, only Apria had the ability to protect its systems (and the Private Information that it stored on them) from attack.

138. Apria's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, and/or misused, as alleged herein.

139. As a result of Apria's ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

140. Apria's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

141. As a result of Apria's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

142. Apria also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

143. As a direct and proximate result of Apria's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

144. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

145. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

146. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Apria to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

147. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

148. Pursuant to Section 5 of the FTCA, Apria had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

149. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., Apria had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

150. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

151. Apria breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

152. Apria also breached its duties to the California Subclass by failing to protect the confidentiality of individually identifiable medical information that it obtained and controlled.

153. Specifically, Apria breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to: proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

154. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, along with the industry-standard cybersecurity measures also set forth above, form part of the basis of Apria's duty in this regard.

155. Apria also violated the FTCA, HIPAA, and the CMIA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

156. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Apria's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

157. Plaintiffs and Class Members are within the class of persons that the FTCA, HIPAA, and the CMIA are intended to protect and Apria's failure to comply with both constitutes negligence *per se*.

158. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Apria's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

159. As a direct and proximate result of Apria's negligence *per se*, Plaintiffs and the Class have and continue to suffer, or are at a substantial and impending risk of suffering, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the actual misuse of their Private Information and the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

160. As a direct and proximate result of Apria's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

161. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Apria to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

162. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

163. Plaintiffs and Class Members entered into a valid and enforceable contract through which money was paid to Apria by them (or on their behalf) in exchange for goods and/or services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

164. Apria's Privacy Policy memorialized the rights and obligations of Apria and its patients. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

165. In the Privacy Policy, Apria commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

166. Plaintiffs and Class Members fully performed their obligations under their contracts with Apria.

167. However, Apria did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore Apria breached its contracts with Plaintiffs and Class Members.

168. Apria allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, Apria breached the Privacy Policy with Plaintiffs and Class Members.

169. Apria's failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, resulted in Apria providing services to Plaintiffs and Class Members that were of a diminished value.

170. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class Members.

171. As a direct and proximate result of Apria's conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

172. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Apria to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

173. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

174. This Count is pleaded in the alternative to Count III above.

175. Apria provides sleep apnea and other breathing care and treatment, wound care, diabetes equipment, and pharmaceutical services to its patients. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those goods and services

through their collective conduct, including through payments made by Plaintiffs and Class Members or on their behalf for goods and services from Defendant.

176. Through Defendant's sale of goods and services, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with its policies, practices, and applicable law and industry standards.

177. As consideration, (a) money was paid by Plaintiffs and Class Members (or on their behalf) to Apria, and (b) Plaintiffs and Class Members turned over valuable Private Information to Apria. Accordingly, Plaintiffs and Class Members bargained with Apria to securely maintain and store their Private Information.

178. Apria accepted possession of the payments and Plaintiffs' and Class Members' Private Information for the purpose of providing goods and services to Plaintiffs and Class Members.

179. In delivering their Private Information to Apria and paying for goods and services, Plaintiffs and Class Members intended and understood that Apria would adequately safeguard the Private Information as part of the services being provided.

180. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and

Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

181. Plaintiffs and Class Members would not have entrusted their Private Information to Apria in the absence of such an implied contract.

182. Had Apria disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Apria.

183. As a provider of healthcare related products and services, Apria recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

184. Apria violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. Apria further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

185. Additionally, Apria breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

186. Apria also breached its implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

187. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

188. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

189. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

190. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

191. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

192. Apria further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

193. Apria further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical

administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

194. Apria further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

195. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete Private Information and to pay Apria in exchange for Apria's agreement to, *inter alia*, protect their Private Information.

196. Plaintiffs and Class Members have been damaged by Apria's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V
INTRUSION UPON SECLUSION / INVASION OF PRIVACY (ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

197. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

198. Plaintiffs and Class Members maintain a privacy interest in their Private Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

199. Plaintiffs and Class Members' Private Information was contained, stored, and managed electronically in Apria's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because highly sensitive, confidential matters regarding Plaintiffs' and Class Members' identities were only shared with Apria for the limited purpose of obtaining and paying for Defendant's services.

200. Additionally, Plaintiffs' and Class Members' Private Information is highly attractive to criminals who can nefariously use such Private Information for fraud, identity theft, and other crimes without the victims' knowledge and consent.

201. Apria's disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Private Information is offensive. Apria's disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties permitted the physical and electronic intrusion into private quarters where Plaintiffs' and Class Members' Private Information was stored.

202. Plaintiffs and Class Members have been damaged by Apria's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT VI
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

203. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

204. This Count is pleaded in the alternative to Counts III and IV above.

205. Plaintiffs and Class Members conferred a benefit on Apria by turning over their Private Information to Defendant and by paying for products and/or services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

206. Upon information and belief, Apria funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs and Class Members.

207. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with

applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Apria.

208. Apria has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

209. Apria knew that Plaintiffs and Class Members conferred a benefit upon it, which Apria accepted. Apria profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

210. If Plaintiffs and Class Members had known that Apria had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

211. Due to Apria's conduct alleged herein, it would be unjust and inequitable under the circumstances for Apria to be permitted to retain the benefit of its wrongful conduct.

212. As a direct and proximate result of Apria's conduct, Plaintiffs and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover

from identity theft; (vi) the continued risk to their Private Information, which remains in Apria's possession and is subject to further unauthorized disclosures so long as Apria fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

213. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Apria and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Apria from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

214. Plaintiffs and Class Members may not have an adequate remedy at law against Apria, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VII
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

215. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

216. In light of the special relationship between Apria and its patients whereby Apria became a guardian of Plaintiffs' and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI), Apria was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members. This benefit included (1) the safeguarding of Plaintiffs'

and Class Members' Private Information; (2) timely notifying Plaintiffs and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where Apria's patients' Private Information was and is stored.

217. Apria had a fiduciary duty to act for the benefit of Plaintiffs and the Class upon matters within the scope of its patients' relationship, in particular to keep the Private Information secure.

218. Apria breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently investigate the Data Breach to determine the number of Class Members affected and notify them within a reasonable and practicable period of time.

219. Apria breached its fiduciary duties to Plaintiffs and the Class by failing to protect their Private Information.

220. Apria breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Apria created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

221. Apria breached its fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

222. Apria breached its fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

223. Apria breached its fiduciary duties to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable,

harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

224. Apria breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR 164.306(a)(2).

225. Apria breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

226. Apria breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR 164.306(a)(94).

227. Apria breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

228. As a direct and proximate result of Apria's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer the harms and injuries alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VIII
BREACH OF CONFIDENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

229. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

230. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Apria and ultimately accessed and acquired in the Data Breach.

231. As a healthcare provider, Apria has a special relationship with its patients, including Plaintiffs and Class Members. Because of that special relationship, Apria was provided with and stored Plaintiffs' and Class Members' Private Information and had a duty to maintain such Information in confidence.

232. Patients like Plaintiffs and Class Members have a privacy interest in personal medical and other matters, and Apria had a duty not to disclose such matters concerning its patients.

233. As a result of the parties' relationship, Apria had possession and knowledge of highly sensitive and confidential PHI and PII belonging to Plaintiffs and Class Members, information that was not generally known.

234. Plaintiffs and Class Members did not consent nor authorize Defendant to release or disclose their Private Information to an unknown criminal actor.

235. Apria breached its duty of confidence owed to Plaintiffs and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Plaintiffs' and Class Members' Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement adequate information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security

program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class members' Private Information to a criminal third party.

236. But for Apria's wrongful breach of its duty of confidence owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

237. As a direct and proximate result of Apria's wrongful breach of its duty of confidence, Plaintiffs and Class Members have suffered and will continue to suffer the injuries alleged herein.

238. It would be inequitable for Apria to retain the benefit of controlling and maintaining Plaintiffs' and Class Members' Private Information at the expense of Plaintiffs and Class Members.

239. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT IX
VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE § 56, *ET SEQ.*
(ON BEHALF OF PLAINTIFF STROFFOLINO AND THE CALIFORNIA SUBCLASS)

240. Plaintiff Stroffolino restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

241. Defendant is a "provider of healthcare" services as defined in Cal. Civ. Code § 56.06 and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

242. Plaintiff Stroffolino and the California Subclass are "patients," as defined in CMIA, Cal. Civ. Code § 56.05(k) ("'Patient' means any natural person, whether or not still living, who received healthcare services from a provider of healthcare and to whom medical information pertains.").

243. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the inactions of Defendant, including its failure to adequately implement sufficient data security and monitoring measures and protocols to protect Plaintiff Stroffolino's and California Subclass Members' Private Information, which allowed hackers to obtain such Information.

244. Specifically, Defendant's negligence resulted in the release of individually identifiable PHI pertaining to Plaintiff Stroffolino and the California Subclass to unauthorized cybercriminals and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff Stroffolino's and California Subclass Members' Private Information in a manner that preserved the confidentiality of the information contained therein is a violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

245. Defendant's systems and protocols did not protect and preserve the integrity of electronic medical information belonging to Plaintiff Stroffolino and the California Subclass, in violation of Cal. Civ. Code § 56.101(b)(1)(A).

246. Plaintiff Stroffolino and the California Subclass were injured and have suffered damages, as described above, from Defendant's illegal disclosure and negligent acts and omissions resulting in the release of their medical information, in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages,

nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs.

COUNT X
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. PROF. CODE § 17200, *ET SEQ.*
(ON BEHALF OF PLAINTIFF STROFFOLINO AND THE CALIFORNIA SUBCLASS)

247. Plaintiff Stroffolino restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

248. Defendant violated California's Unfair Competition Law ("UCL") Cal. Bus. Prof. Code § 17200, et seq., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. By representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff Stroffolino's and California Subclass Members' Private Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that Defendant would and did comply with the requirement of relevant federal and state laws relating to privacy and security of Plaintiff Stroffolino and California Subclass Members' Private Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Private Information;

b. By soliciting and collecting Private Information from Plaintiff Stroffolino and California Subclass Members without adequately protecting or storing Private Information;

c. By violating the privacy and security of HIPPA, 42 U.S.C. §1302d, *et seq*.; and

d. By violating the CMIA, Cal. Civ. Code § 56, *et seq*.

249. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities that solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq*., and the CMIA, Cal. Civ. Code § 56, *et seq*.

250. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff Stroffolino and the California Subclass were injured and lost money and property, including but not limited to, the loss of their legally protected interest in the confidentiality and privacy of their Private Information, including PHI, and additional losses described above.

251. Defendant knew or should have known that its data security practices, procedures, and protocols were inadequate to safeguard Plaintiff Stroffolino's and California Subclass Members' Private Information and that the risk of theft was highly likely. Defendant had resources to secure and/or prepare for protecting patient Private Information in a Data Breach. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

252. Plaintiff Stroffolino seeks, on behalf of herself and the California Subclass, relief under the UCL, including restitution to the Class of money or property that Defendant may have acquired by means of its deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

COUNT XI
VIOLATION OF CALIFORNIA'S CUSTOMER RECORDS ACT
(ON BEHALF OF PLAINTIFF STROFFOLINO AND THE CALIFORNIA SUBCLASS)

253. Plaintiff Stroffolino restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

254. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

255. Defendant is a business that maintains PII pertaining to Plaintiff Stroffolino and California Subclass Members within the meaning of Cal. Civ. Code § 1798.81.5, including Social Security numbers, as alleged herein.

256. Businesses that maintain computerized data that includes PII are required to "notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

257. Defendant is a business that maintains computerized data that includes PII as defined by Cal. Civ. Code § 1798.80.

258. Plaintiff Stroffolino's and California Subclass Members' PII includes Personal Information as covered by Cal. Civ. Code § 1798.82.

259. Because Defendant reasonably believed that Plaintiff Stroffolino's and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach, immediately following its discovery, to the owners or licensees of the PII (*i.e.*, Plaintiff Stroffolino and the California Subclass Members) as mandated by Cal. Civ. Code § 1798.82.

260. By failing to disclose the Data Breach immediately following its discovery, Defendant violated Cal. Civ. Code § 1798.82.

261. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff Stroffolino and California Subclass Members suffered damages, as described above, and as will be proven at trial.

262. Plaintiff Stroffolino and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT XII
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("CFA")
(ON BEHALF OF PLAINTIFF SMITH AND THE ILLINOIS SUBCLASS)

263. Plaintiff Smith restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

264. Plaintiff Smith and the Illinois Subclass are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff Smith, the Illinois Subclass, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

265. Defendant is engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

266. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their medical equipment and services, in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff Smith's and the Illinois Subclass's sensitive PII and PHI from being stolen by cybercriminals, and failing to comply with applicable state and federal laws

and industry standards pertaining to data security, including the FTCA and HIPAA; (2) failing to disclose, or omitting, material facts to Plaintiff Smith and the Illinois Subclass regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII and PHI of Plaintiff Smith and the Illinois Subclass; (3) failing to disclose, or omitting material facts, to Plaintiff Smith and the Illinois Subclass about its failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII and PHI of Plaintiff Smith and the Illinois Subclass; and (4) failing to take proper action following the Data Breach to enact adequate notice, privacy and security measures and protect Plaintiff Smith and the Illinois Subclass's PII and PHI and other personal information from further unauthorized disclosure, release, data breaches, and theft.

267. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and such failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff Smith and the Illinois Subclass, and thus would defeat their reasonable expectations about the security of their PII and PHI.

268. Defendant intended that Plaintiff Smith and the Illinois Subclass rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with its offering of goods and services.

269. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Illinois Subclass. Plaintiff Smith and the Illinois Subclass have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

270. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff Smith and the Illinois Subclass of the nature and extent of the Data Breach, pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, et seq.

271. As a result of Defendant's wrongful conduct, Plaintiff Smith and the Illinois Subclass were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's products and/or services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII and PHI from being accessed, viewed, taken and/or misused by others.

272. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff Smith and the Illinois Subclass have suffered and/or at a continuous, substantial and imminent risk of suffering, harm that includes but is not limited to the actual misuse of their Private Information; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant by or on the behalf of Plaintiff Smith and Illinois Subclass Members that would not have been made had they known of Defendant's inadequate data security; lost control over the value of their PII and PHI; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

273. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff Smith and the Illinois Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

COUNT XIII
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

274. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

275. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

276. Apria owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

277. Apria still possesses Private Information regarding Plaintiffs and Class Members.

278. Plaintiffs allege that Apria's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

279. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Apria owes a legal duty to secure its patients' Private Information and to timely notify them of a data breach under the common law, HIPAA, the FTCA, and the state statutes invoked herein;

b. Apria's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect patients' Private Information; and

c. Apria continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

280. This Court should also issue corresponding prospective injunctive relief requiring Apria to employ adequate security protocols consistent with legal and industry standards to protect patients' Private Information, including the following:

a. Order Apria to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Apria must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Apria's systems on a periodic basis, and ordering Apria to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Apria's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps Apria's patients should take to protect themselves.

281. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Apria. The risk of another such breach is real, immediate, and substantial. If another breach at Apria occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

282. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Apria if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Apria's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Apria has a pre-existing legal obligation to employ such measures.

283. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Apria, thus preventing future injury to Plaintiffs and other patients whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class and State Subclasses requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Apria to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Apria to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: June 12, 2023

Respectfully submitted,

/s/ *Kathleen A. DeLaney*

Kathleen A. DeLaney (#18604-49)
DELANEY & DELANEY LLC
3646 North Washington Blvd.

Indianapolis, IN 46205
Tel: 317-920-0400
E: kathleen@delaneylaw.net

SIRI & GLIMSTAD LLP
Mason A. Barney (*pro hac vice* to be filed)
Tyler J. Bean (*pro hac vice* to be filed)
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com